Universidade Gama Filho

Utilização de *honeypot* e estudo comportamental de invasores na administração da segurança em redes

Brasília

2010

BDJur
http://bdjur.stj.gov.br

Alan Alves Araújo

Utilização de *honeypot* e estudo comportamental de invasores na administração da segurança em redes

BDJur
http://bdjur.stj.gov.br

Alan Alves Araújo

Segurança de redes

Trabalho de Conclusão de Curso

Trabalho de Conclusão de Curso apresentado ao
Programa de Ensino à Distância
Universidade Gama Filho

Utilização de *honeypot* e estudo comportamental de invasores na administração da segurança em redes.

Orientador: Prof. Júlio Noguchi

Brasília
2010

BDJur
http://bdjur.stj.gov.br

FOLHA DE APROVAÇÃO DA MONOGRAFIA

UNIVERSIDADE GAMA FILHO
CURSO DE PÓS-GRADUAÇÃO LATO SENSU
SEGURANÇA DE REDES DE COMPUTADORES
UTILIZAÇÂO DE *HONEYPOT* E ESTUDO COMPORTAMENTAL DE INVASORES NA ADMINISTRAÇÃO DE SEGURANÇA EM REDES
Esta monografia será examinada e aprovada para a obtenção do título de Especialização em Segurança de Redes de Computadores no Programa de Pós-Graduação da Universidade Gama Filho

_____
Prof. Julio Celso Noguchi – Orientador

_____
Examinador

_____
Examinador
[BRASILIA/DF]
[2010]

BDJur
http://bdjur.stj.gov.br

LISTA DE ILUSTRAÇÕES

Figura 2.3.1 – Técnica de *Footprint* utilizando a INTERNIC para acessar informações do site www.enom.com

Pag. 19

Figura 2.3.2 – Varredura utilizando o comando *ping.*

Pag. 21

Figura 2.3.2.2 – Varredura utilizando o programa *nmap*.

Pag. 22

Figura 2.3.5 – *Spoofing* utilizando o programa *Sterm*.

Pag. 28

Figura 2.3.5.1 – Configurando IP e porta no *Sterm* para *Spoofing*.

Pag. 29

Figura 2.3.5.2 – Resultado do *Spoofing* usando *Sterm*.

Pag. 30

Figura 4.2.3 – Localização do *Hoenypot* na rede.

Pag. 38

BDJur
http://bdjur.stj.gov.br

LISTA DE ABREVIATURAS E SIGLAS

DMZ - DeMilitarized Zone ou "zona desmilitarizada"
VPN - Virtual Private Network
IDS - Intrusion detection system
HTTP - Hypertext Transfer Protocol
FTP - File Transfer Protocol
LAN - Local area network
WAN - Wide area network
SMPT - Simple Mail Transfer Protocol
POP3 - Post Office Protocol
IMAP - Internet Message Access Protocol
TMRC - Tech Model RailRoad Club
INTERNIC - Internet Network Information Center
TCP/IP - Transmission Control Protocol/Internet Protocol
DNS - Domain Name System
MAC - Media Access Control
ARP - Address Resolution Protocol
IP - Internet Protocol
ICMP - Internet Control Message Protocol
UDP - User Datagram Protocol
SSH - Secure Shell
DHCP - Dynamic Host Configuration Protocol

BDJur
http://bdjur.stj.gov.br

SUMÁRIO

TEMÁTICA E PROBLEMA 8

OBJETIVOS 9

CAP. I SEGURANÇA DE REDES 11

CAP. II *HACKERS* 17

CAP. III PROCESSO COGNITIVO 33

CAP. IV UTILIZAÇÃO DE HONEYPOT 36

CONCLUSÃO.....43

REFERENCIAL BIBLIOGRÁFICO.....45

BDJur
http://bdjur.stj.gov.br

Tema:

Segurança de Redes

Delimitação do Tema

Controle social em segurança de redes

Problematização

Como a utilização de "*Honeypot*" cognitivo pode contribuir para entender e controlar o comportamento *hacker* na segurança de redes.

Referencial Teórico

Sobre o assunto Segurança de redes farei uso da seguinte literatura:
-Winters,scott. Northcutt,Stephen.Frederick,Karen.Zeltser,Lenny.Ritchey,Ronald W.- Desvendando Segurança de Redes . Ed. Campos . São Paulo - 2002

Sobre o assunto utilização de *Honeypot* utilizarei farei uso principalmente da seguinte literatura:
-Assunção, Marcos Flávio Araújo. *Honeypots e Honeynets-Aprenda a detectar e enganar invasores. Ed. Visual Books. São Paulo-2009*.

Para tratar do assunto referente ao processo cognitivo farei uso da seguinte literatura como norteador dos trabalhos:
- Foucault, Michel. *As palavras e as coisas. Ed Martins. São Paulo. 2007*. O livro aborda como o processo cognitivo surge das sucessivas classificações por similaridade que a sociedade produz ao longo de sua história.

Para analisarmos o comportamento *hacker* farei uso de:

BDJur
http://bdjur.stj.gov.br

-Assunção, Marcos Flávio Araújo . *Segredos do Hacker Ético.Ed. Visual Books – São Paulo, 2010,* Neste livro o autor expõe as técnicas e comportamento dos *Hackers*.

Justificativas.

De acordo com as informações disponibilizadaspelo *Honeypot* será possível ao administrador de segurança conhecer as ações executadas pelo *Hacker* e implementar medidas que contenham os ataques econtrolem o comportamento daqueles atacantes.

Objetivos

Geral:

Oferecer à Segurança de redes uma simulação de serviço (honeypot) que possibilite ao administrador, através de parâmetros cognitivos, entender,antever e controlar o comportamento *hacker*.

ObjetivosEspecíficos

-Mostrar as vantagens da utilização de *Honeypot* como técnica de segurança.
-Identificar os principais ataques em redes e o comportamento *Hacker*.
-Apresentar como o processo cognitivo pode oferecer elementos de mudança comportamental de *Hackers*.

BDJur
http://bdjur.stj.gov.br

Descrição dos Capítulos

1. Segurança de Redes. Neste capítulo descreverei os diversas técnicas existentes na atualidade para a Segurança de redes.

2. *Hackers* – Neste capítulo irei expor os principais ataques utilizados pelos Hackers bem como as motivações deste comportamento.

3. Processo cognitivo – Neste capítulo irei dissertar sobre como o processo cognitivo pode ser entendido pelos administradores de segurança no sentido de orientar as técnicas de contenção e controle do comportamento *hacker* pernicioso.

4. Utilização de *honeypot* – Neste capítulo irei mostrar uma solução de implementação de um ambiente virtual (*honeypot*) que possibilite ao administrador, além de monitorar o comportamento *hacker*, reconfigurar o sistema direcionando novos ataques à uma mudança comportamental.

BDJur
http://bdjur.stj.gov.br

Capitulo 1 — Segurança de Redes

O tema segurança de redes por muito tempo é discutido nas empresas e no meio técnico-acadêmico por representar uma preocupação de toda a sociedade no que se refere à proteção aos ativos e sistemas de informação. A equipe responsável pela manutenção dos recursos computacionais que ofereçam uma segurança de redes efetiva necessita de estar sempre atualizada com as melhores práticas e técnicas existentes nas organizações para que os ativos estejam sempre protegidos de ataques. O mercado de informática e as comunidades livres na internet fornecem ferramentas de controle, análise e diagnóstico de segurança que podem ser de extrema utilidade aos administradores de segurança. Mas é necessário, além disso, que a equipe tenha um treinamento específico para algumas ferramentas para que todo o processo de se manter uma rede segura seja otimizado. Profissionais especializados em determinada técnica de bloqueio de invasão como Firewalls por exemplo possibilitam uma resposta imediata aos ataques nas redes de comunicação. Para entendermos a segurança de redes necessitamos explicitar o conceito de perímetro, o perímetro, segundo NORTHCUTT:5, "é a borda fortificada de nossa rede, que pode incluir o seguinte:

- Roteadores
- Firewalls
- IDS
- Dispositivos de VPN
- Software
- DMZs *e screened subnets*"

Os Roteadores são os primeiros elementos de um perímetro, Segundo IGDUCA os roteadores "são os responsáveis, entre outras funções, por enviar pacotes de 1dados (mensagens, arquivos etc.) não só pela internet, mas também por outras redes, escolhendo o melhor caminho entre os milhões disponíveis para interligar dois computadores. Um exemplo para ilustrar: ao apertar o botão 'Enviar' em seu programa de e-mails, como é possível garantir que a

BDJur
http://bdjur.stj.gov.br

mensagem chegará ao destinatário correto, entre os muitos disponíveis? Grande parte deste trabalho é feita pelos roteadores. As pequenas redes domésticas são um exemplo de sua utilização, mas os roteadores estão presentes em empresas de todos os tamanhos (pequenas, médias e até gigantes) e com múltiplas funções."

Os Firewalls são elementos de segurança em redes utilizados para filtrar e bloquear o tráfego indesejado. Antes de entendermos o conceito de roteador precisamos definir o que é Proxy - PROXY: "O serviço de proxy consiste em manter, em uma área de acesso rápido, informações já acessadas por outro usuário, evitando assim a retransmissão destas informações e deixando-as disponíveis ao usuário num tempo bem menor... sempre que há uma requisição de serviços HTTP ou FTP, o servidor proxy captura os dados que o servidor web disponibiliza ao cliente (usuário) e os guarda em uma área em disco. Na próxima vez que este *site* for acessado, o *navegador* primeiro fará a procura no servidor proxy. Se os dados forem encontrados neste servidor, a transferência de dados se dará entre ele e o cliente (*navegador*). Se o servidor proxy não dispuser dos dados requisitados, o acesso será feito diretamente ao *site* de destino". NORTHCUTT:5 expõe que "Um firewall é um dispositivo que possui um conjunto de regras especificando que tráfego ele permitirá ou negará. Um firewall determina onde finaliza o roteador e cria uma passagem muito mais detalhada no tráfego de filtragem. Existem vários tipos de firewall diferentes, incluindo filtros de pacote estático, firewalls com estado e firewalls Proxy. Você poderia usar um filtro de pacote estático, com um roteador Nortel Accellar, para bloquear uma sub-rede, um firewall com estado, como o cisco PIX, para controlar serviços permitidos ou um firewall Proxy, como o Sidewinder da Secure Computing, para controlar o conteúdo. Embora os firewalls não sejam perfeitos, eles bloqueiam aquilo que dizemos para bloquear e permitem o que dizemos para permitir."

Os IDS (Intrusion Detection System) são ferramentas de administração em segurança de redes que possibilitam aos administradores detectar possíveis ataques na rede- IDSRNP – "O sistema de detecção de intrusão ou IDS, tem como um dos objetivos principais detectar se alguém está tentando entrar no seu sistema ou se algum usuário legitimo está fazendo mau uso do mesmo. Esta ferramenta roda constantemente em background e somente gera uma notificação quando detecta alguma coisa que seja suspeita ou ilegal".

Dispositivos de VPN (Virtual Private Network), são elementos específicos para comunicação privada entre um acesso externo e a rede interna. NORTHCUTT:5 – "Uma VPN é uma sessão de rede protegida formada através de canais desprotegidos, como a Internet. Freqüentemente, fazemos referência a uma VPN em função do dispositivo no perímetro que permite a sessão criptografada, como um Nortel Contivity. O uso pretendido pode ser para parceiros de negócios, policiais rodoviários ou tele comutadores. Uma VPN permite que um usuário externo participe na rede interna como se estivesse conectado diretamente a ela. Muitas organizações têm um falso senso de segurança em relação ao seu acesso remoto porque possuem uma VPN. Se um

BDJur
http://bdjur.stj.gov.br

atacante comprometer a máquina de um usuário legítimo. Uma VPN pode fornecer a esse atacante um canal criptografado para dentro de sua rede. Você pode confiar na segurança do seu perímetro, mas você confia na segurança de um de seus tele comutadores em um modem a cabo em casa ou discando em um quarto de hotel ? Mesmo que confie neles e em sua segurança, você pode confia na segurança, você pode confiar na segurança dos usuários de acesso remoto do seu parceiro conectado à VPN ?". Ainda sobre VPN, NORTHCUTT : 181 – " Uma VPN é uma conexão que é estabelecida por uma infra-estrutura "pública" ou compartilhada existente, usando tecnologias de criptografia ou autenticação para proteger seu payload. Isso cria um segmento 'virtual' entre duas entidades quaisquer que têm acesso. Isso poderia ocorrer pela infra-estrutura compartilhada de uma rede local (LAN), conexões WAN ou internet."

Os softwares são programas de computador que estão presentes na rede. A administração de segurança em redes deve ter um cuidado especial com esses elementos pois a partir de uma instalação ou adulteração de um código ou arquivo de software um atacante pode ter acesso aos recursos e ativos internos da rede. NORTHCUTT:6 – " Arquitetura de Software se refere às aplicações que são hospedadas na rede da empresa e define como elas são estruturadas. Por exemplo, poderíamos estruturar uma aplicação de comércio eletrônico dividindo-a em três camadas distintas:

- O front-end da Web, que é responsável pela forma como aplicação é apresentada ao usuário
- O código de aplicação, que implementa a lógica comercial da aplicação
- Os bancos de dados de back-end, que armazenam dados fundamentais para a aplicação

A arquitetura de software desempenha um papel importante na análise de uma infra-estrutura de segurança porque a principal finalidade do perímetro da rede é proteger os dados e os serviços da aplicação. Ao proteger a aplicação, assegure-se de que a arquitetura do software e a rede estejam em harmonia."

As DMZs são redes separadas logicamente ou fisicamente com finalidade de proteger os ativos de rede. DMZREF: "È a sigla para de DeMilitarized Zone ou "zona desmilitarizada", em português. DMZ é uma pequena rede situada entre uma rede confiável e uma não confiável, geralmente entre a rede local e a Internet.

BDJur
http://bdjur.stj.gov.br

Segundo NORTHCUTT, A função de uma DMZ é manter todos os serviços que possuem acesso externo (tais como servidores HTTP, FTP, SMPT, POP3, IMAP e etc.) separados da rede local, limitando assim o potencial dano em caso de comprometimento de algum destes serviços por um invasor. Para que esse objetivo seja atingido os computadores presentes em uma DMZ não contem nenhuma forma de acesso à rede local. A configuração é realizada através do uso de equipamentos de Firewall, que vão realizar o controle de acesso entre a rede local, a Internet e a DMZ (ou, em um modelo genérico, entre as duas redes a serem separadas e a DMZ). Os equipamentos na DMZ podem estar em um switch dedicado ou compartilhar um switch da rede, porém neste último caso devem ser configuradas Redes Virtuais distintas dentro do equipamento, também chamadas de vlans (Ou seja, redes diferentes que não se “enxergam” dentro de uma mesma rede - LAN).

O método mais simples de criar uma DMZ é utilizar um firewall com três ou mais

Interfaces de rede. A cada interface é atribuído um papel específico:

1.Rede interna confiável

2.Rede DMZ

3.Não confiável rede externa (Internet)

Com uma porta utilizando uma placa Ethernet no seu firewall irá permitir que você crie uma rede nesta configuração, ou até mesmo permitir que você crie uma rede com duas distintas da DMZ. Separar o DMZ em múltiplos hosts da DMZ irá ajudar a limitar os danos que pode ser feito se um de seus hospedeiros DMZ está comprometida. Se for utilizar uma DMZ com regras de Firewall, o Firewall será normalmente configurado para proteger a rede interna da Internet. Para criar uma DMZ, o firewall também deve aplicar as regras para proteger o DMZ a partir da Internet e das regras destinadas a proteger a rede interna da DMZ. Isto tornará mais difícil para um atacante para penetrar a rede interna.

BDJur
http://bdjur.stj.gov.br

Devemos pensar a segurança de redes como uma cebola, em camadas "Quando você descasca a camada mais externa, muitas camadas permanecem por baixo dela. Nenhum conceito transmite mais importância ao discutirmos segurança de rede do que o da defesa em profundidade. A defesa em profundidade o ajuda a proteger recursos de rede mesmo que uma das camadas de segurança esteja comprometida . Afinal, nenhuma camada de segurança pode garantir que resistirá a cada ataque que tenha que enfrentar"- NORTHCUTT: 7 .

As camadas de segurança numa rede de informações dependem em muito dos valores e riscos envolvidos no ambiente. Uma análise de riscos deve ser feita pela equipe de segurança para determinar quais ativos deverão ser protegidos e quantas camadas de segurança serão necessárias para essa proteção. Assim os ambientes devem ser segurados segundo a classificação dos ativos na rede. Serviços externos, por exemplo, devem estar mais próximos à ultima camada do perímetro de forma a facilitar o acesso dos usuários. Um servidor de páginas web deve estar posicionado em uma camada de segurança que possibilite o acesso externo. As camadas mais externas do perímetro devem estar bem protegidas e com tráfego de rede bem monitorado e filtrado para não comprometer a segurança das camadas mais internas. Outro conceito importante em segurança de redes são os castelos, os castelos segundo NORTHCUTT:588 "...geralmente possuem um controle de perímetro que inclui um meio de entrar e sair. Os castelos também usam pontos de estrangulamento. É fácil ver a ação da defesa em profundidade; para resgatar a princesa na torre, você precisa atravessar o fosso e baixar o grande portão. Depois, você está em uma área com portas falsas, semelhantes a uma câmara de compressão, portas de controle externo, uma área de reunião e um conjunto interior de portas, e somente um conjunto de portas deverá abrir de cada vez. Assim, mesmo que você penetre por um conjunto de portas, terá que entrar na área de reunião, onde haverá portas por onde o pessoal interno poderá atirar em você, e outro conjunto de portas para prosseguir." Podemos empregar muitos elementos da arquitetura do castelo em nossas redes. Os roteadores de borda e firewalls são usados da mesma forma que os fossos e portas falsas. O castelo não é invencível, mas a arquitetura de defesa em profundidade deve ser cuidadosamente considerada. Os castelos não estão mais em uso militar atualmente, pois tinham vários problemas que se relacionam a moderna defesa do perímetro. Os canhões eram um grande problema. Portas dos fundos e passagens secretas faziam mais do que permitir a entrada no castelo, e como eram fixos e fáceis de se encontrar, essa era uma desvantagem significativa. Com nossas redes, temos problemas semelhantes. Pontos de acesso e modems sem fio, especialmente na resposta automática, são as portas dos fundos e as passagens

BDJur
http://bdjur.stj.gov.br

secretas de nossas redes. Os sites com espaços de endereços públicos, como os castelos, são expostos, fixos e fáceis de se encontrar e atacar.

Uma arquitetura de segurança do perímetro deve ser implementada de acordo com cada organização. As práticas e técnicas em segurança de redes irão variar dependendo dos ativos e dos respectivos riscos envolvidos na administração. Faz-se necessário que a organização formule uma política de segurança da informação. NORTHCUTT: 99 - "Uma política de segurança estabelece o que precisa ser feito para a proteção das informações armazenadas nos computadores. Uma política bem escrita contém a definição suficiente do 'que' fazer de modo que o 'como' possa ser identificado e medido ou avaliado". A política pode ser imposta ou não. A utilização de um Firewall, por exemplo, é uma política de imposição. Na política sem imposição o administrador utiliza-se de elementos de persuasão, mas sem impor uma regra ou norma.

BDJur
http://bdjur.stj.gov.br

Capitulo 2 — *Hackers*

2.1 O termo *Hacker*

O termo *Hacker* MICHAELIS: 95 “Pessoa viciada em computadores, com conhecimentos de informática, que utiliza esse conhecimento para o benefício de pessoas que usam o sistema, ou contra eles”, OXFORD “*use a computer to gain unauthorized access to data* – Uso do computador para efetuar um acesso não autorizado aos dados”, como podemos perceber, é visto pelo público em geral como algo similar a contraventor, criminoso. No entanto segundo ARAUJO:7 – “O termo *hacker* foi introduzido a informática aproximadamente na década de 1960, para designar pessoas que conseguiam resolver problemas comuns de formas incomuns. E é geralmente esse o conceito central: a criatividade. Isso é o que separa um *hacker* de um profissional da mesma área, seja ele qual for. Como se fossem dois mecânicos: um acredita que precisa trocar uma peça do carro, outro usa a cabeça e pensa em uma maneira alternativa para resolver o problema, usando os recursos que já possui.” A criatividade é característica essencial ao se definir o conceito de *Hacker*. O processo criativo está intimamente ligado ao processo cognitivo, mais adiante iremos aprofundar esta relação, mas podemos conceituar o termo *Hacker* como o indivíduo criativo, ou vulgarmente conhecido como “fuçador”, aquele que tem a curiosidade e vontade de aprender. O aspecto criminal e contraventor existente no imaginário popular está mais relacionado ao que a mídia divulga do que efetivamente no comportamento dos *hackers*.

Já PEDROSO:95 nos traz a etimologia do termo : “Etimologicamente o termo *Hacker* está relacionado ao verbo cortar nas línguas germânicas. O termo desenvolveu-se vindo a ser associado ao ato de modificar ou inventar algo para realizar funcionalidades que não as originais. As atividades criativas e originais de um inventor ou mecânico seriam o equivalente de hacking, "hackear" na língua portuguesa”.

PEDROSO nos diz ainda que o termo é ligado como vimos ao fator criativo, mas surgiu dentro da comunidade técnica, A palavra "hack" nasceu num grupo chamado Tech Model RailRoad Club (TMRC) na década de 50. Membros do clube (soldier e ChAoS) chamavam as modificações inteligentes que faziam nos relês eletrônicos de 'hacks'. Quando as máquinas TX-0 e PDP-1 chegaram ao mercado os membros do TMRC começaram a utilizar o mesmo jargão para descrever o que eles estavam fazendo com a programação de computadores. Isso continuou por anos até mesmo quando novas máquinas como o PDP-6 e depois o PDP-10 apareceram. O

BDJur
http://bdjur.stj.gov.br

termo passou a ser usado com diversos significados: sucessos em determinadas áreas, fosse como uma solução não óbvia e particularmente elegante para um problema, ou uma partida inteligente pregada a alguém, ou ligar os sistemas informáticos e telefônicos para fazer chamadas grátis. Eventualmente, o termo passou a ser utilizado exclusivamente nas áreas da programação ou eletrônica, em que passou a ser usado para designar indivíduos que demonstravam capacidades excepcionais nestes campos, efetivamente expandindo-os com atividades práticas e artísticas. Esse aspecto técnico do termo faz surgir no imaginário coletivo a falsa imagem de que a pessoa que comete crime computacional possui uma formação técnica de alto nível. Percebemos que os delinqüentes, apesar de serem inteligentes, não possuem formação técnica na área de informática.

2.2 Comportamento *Hacker*

Porque a maioria dos profissionais de segurança em redes, que quase sempre possuem um conhecimento técnico mais avançado que o dos *Hackers*, não conseguem antever os ataques e técnicas utilizadas pelos *Hackers* ? A resposta é simples, o processo cognitivo do *hacker* é completamente diferente do processo cognitivo acadêmico dos técnicos. A intuição de um *hacker* é extremamente mais aguçada se compararmos com a de um técnico. O fator da criatividade volta a ser o elemento divisor de águas, o *Hacker* mantém-se em liberdade criativa enquanto o técnico está “preso” a normas, procedimentos e padrões. Temos um bom exemplo dessa disparidade: ARAUJO:7 - “ Exemplos interessantes podem ser notados em tecnologias anti-cópias de Cds de áudio. Após um investimento de centenas de milhares de dólares em um novo sistema seguro, descobriu-se que ele poderia ser burlado apenas com a utilização de uma fita adesiva colada nas bordas do disco.Outro Caso: conseguiram, através de um sistema complexo de certificação, impedir que um programa copiasse as músicas do CD para o disco. Solução simples: ligue a saída de som do micro system, na entrada de áudio do PC.”

BDJur
http://bdjur.stj.gov.br

2.3 Ataques

2.3.1 Footprinting

A técnica de *Footprinting* é utilizada pelos *Hackers* com o objetivo de obter informações sobre a rede e os sistemas alvos do ataque. GRUPOCSI – "Footprinting é a arte de obter informações sobre um sistema alvo usando táticas 'seguras', sem perigo de detecção, e que pode dar muitas informações sobre ele. Tais como visitar o site da empresa em que se quer invadir e ler as seções para ver se encontra algo de interessante. O footprinting é o nome dado ao ato de realizar comandos remotos ao alvo, ou sistema remoto, com objetivo de recolher informações tais como, qual Sistema Operacional usa, quais portas ficam abertas para entrada, qual sistema de defesa usa, entre outros". Um dos elementos mais utilizados pelos *Hackers* para a pesquisa de *footprinting* é a consulta direta na internet, alguns sites como o WWW.registro.br e WWW.INTERNIC.net, por exemplo, fornecem informações valiosas, tais como o endereço IP do servidor da empresa na internet, para um ataque, abaixo temos um resultado de uma pesquisa no site da "INTERNIC" que retorna informações dos servidores DNS do endereço da internet:

Figura 2.3.1 – Técnica de Footprint utilizando a INTERNIC para acessar informações do site www.enom.com

BDJur
http://bdjur.stj.gov.br

Além desta forma de pesquisa o atacante pode utilizar de ferramentas de pesquisa automática. ARAUJO:38 "Nesse tipo de pesquisa, utiliza os ferramentas automáticas que possa descobrir informações úteis sobre qualquer alvo. Esses programas podem realizar operações como: filtrar pesquisas nos websites, descobrir endereços de e-mails, arquivos da instalação de alguns softwares esquecidos, traçar rotas até o alvo, consultar o seu domínio e diversas outras tarefas que tenha o intuito de lhe ensinar mais sobre o seu alvo". Outro recurso muito utilizado pelos *Hackers* para obter informações sobre seu alvo é a pesquisa em sites especializados como o Google. As páginas de busca podem fornecer recursos de pesquisa de informações com alto nível de profundidade e com possibilidade de catalogar as páginas que encontra, exemplo de consulta: *+inurl : admin +"Indexo f /admin"*, essa consulta irá retornar uma lista de arquivos dentro do diretório admin.

2.3.2 Varreduras

A varredura ("*scanning*") é uma técnica utilizada pelos atacantes para descobrir quais sistemas estão ativos na rede e de que maneira eles podem ser acessados. Geralmente, um sistema é disponibilizado na rede através do protocolo TCP/IP, esse protocolo disponibiliza uma "porta" de acesso ao sistema, a varredura é feita buscando quais portas TCP/IP estão abertas e disponíveis para acessar os sistemas. ARAUJO:45 "...varredura é feita com o intuito de se descobrir computadores ativos em uma determinada rede e quais portas esses sistemas estão rodando. Tentaremos descobrir também quais os serviços que estão vinculados às portas e, se possível, qual o sistema operacional da máquina.Isso pode ser feito manualmente ou usando ferramentas específicas, chamadas de Scanners". Uma das técnicas mais utilizadas para varredura é o "ping": Trata-se de um comando executado que testa a comunicação com outra máquina. Assim o *Hacker* sabe se determinada máquina está ativa ou não. Segue abaixo uma tela de retorno de um comando *ping*:

BDJur
http://bdjur.stj.gov.br

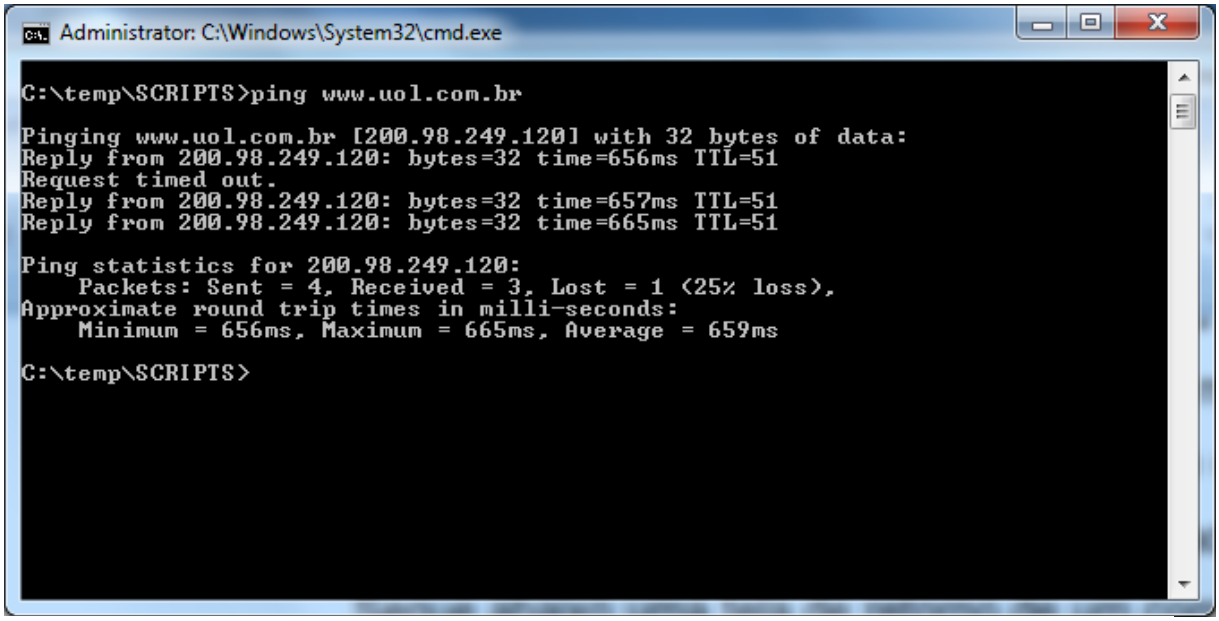

Figura 2.3.2 – Varredura utilizando o comando ping

A linha: *Reply from* 200.98.249.120: *bytes=32 time=657ms TTL=51*, indica que a comunicação com o servidor do site *www.uol.com.br* foi possível.

Após a descoberta de quais computadores estão ativos o *Hacker* procura por quais portas TCP/IP estão ativas em determinado computador. Para isso os atacantes utilizam de ferramentas de varredura específicas como o NMAP: ARAUJO-47 “Criado por Fyodor, esse programa é o scanner mais conhecido de todos, extremamente poderoso e cheio de recursos. Utilizado por dez entre dez *hackers* como parte de seus ataques”. O comando nmap <endreço ip> retorna os números de portas, seu estado(se estão abertas ou filtradas por firewall) e, ainda, uma possível descrição do serviço que está rodando naquela porta:

BDJur
http://bdjur.stj.gov.br

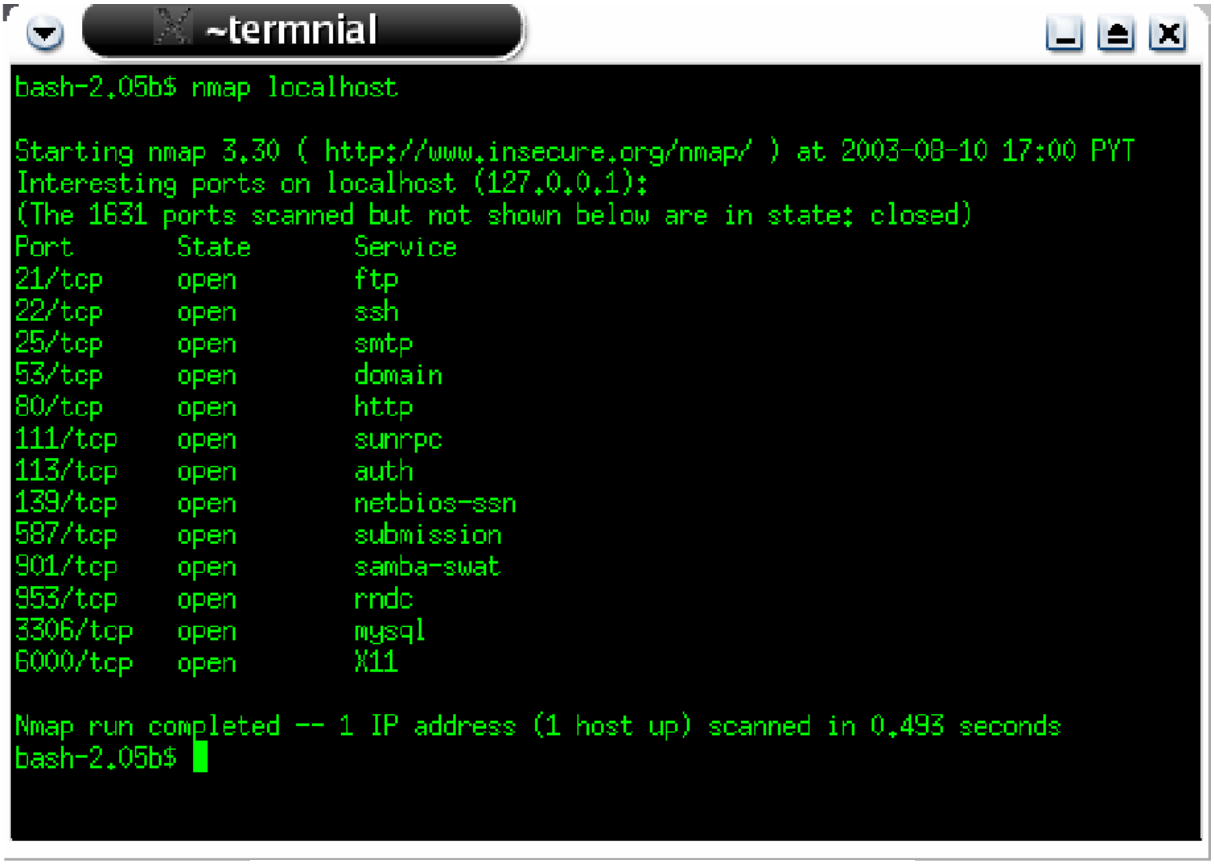

Figura 2.3.2.2 – Varredura utilizando o programa nmap.

2.3.3 Enumeração

A técnica de enumeração geralmente é utilizada após as fases de *footprinting* e varredura. Na enumeração o *Hacker* irá elencar quais serviços estão disponibilizados e em quais portas TCP/IP. A descoberta de qual sistema operacional está rodando no computador alvo, na maioria das vezes, é realizada com essa técnica. ARAUJO:52 " A enumeração é o passo seguinte à varredura. Já temos em nosso poder hosts ativos na rede e as portas que estão abertas nesses sistemas. Mas quais serviços essas portas estão rodando? Qual o sistema operacional do alvo? Será que podemos conseguir extrair nomes de usuários em alguns desses serviços? Todas essas perguntas serão respondidas nessa etapa, a de enumerar os recursos para o passo seguinte". Para se descobrir o Sistema operacional uma das técnicas mais usadas na fase de enumeração é o Fingerprint. Essa técnica consiste em descobrir a informação desejada verificando-se os pacotes de comunicação TCP/IP. O 'OS FingerPrint' (Operation System FingerPrint), como o próprio nome já diz, se refere a impressão digital do sistema operacional.Ele se baseia no fato de que todos os sistemas

BDJur
http://bdjur.stj.gov.br

operacionais, assim como as pessoas, têm características únicas, que podem ser usadas para identificá-los.Assim como os seres humanos podem ser identificados pela íris, pelo ‘polegar’ ou pela face, os sistemas operacionais podem ser identificados por algumas peculiaridades presentes no cabeçalho dos pacotes transmitidos por eles. Para detectar essas diferenças, alguns métodos foram criados, como o ‘Active FingerPrinting’, no qual se envia vários pacotes mal formados e se analisa a resposta fornecida pelo sistema. Geralmente, cada sistema operacional responde de uma maneira diferente a esses pacotes.

2.3.4 Explorando Falhas

Os sistemas digitais e softwares em geral são desenvolvidos de forma a minimizar as falhas de segurança. Uma falha de segurança em um sistema é um ponto da rotina do software em que um atacante pode obter vantagens para efetuar um ataque. Muita das vezes essas falhas são descobertas após o ataque, o desenvolvedor não tem como prever toda a criatividade do *Hacker* ao produzir o sistema. As falhas podem ser locais ARAUJO:62 “Falhas locais é um tipo de falha que só pode ser explorada localmente no sistema, ou seja, um invasor precisaria estar fisicamente usando esse computador ou já possuir acesso local pela internet. Geralmente, as falhas locais são utilizadas para elevação de privilégios.” ou remotas ARAUJO:62 “Esse tipo de falha acontece em servidores que escutam conexões externas. Um daemon/serviço do servidor, como FTP,Web,POP3,SMTP,SMB/NetBIOS, Universal Plug and Play, X11 etc. Como esses serviços fornecem acesso à Internet e, em quase 90% dos casos, eles requerem algum tipo de autenticação, podem vir a ter problemas no caso de alguma falha ser encontrada. Se utilizarmos, por exemplo, uma falhano servidor Web IIS 5.o ou Apache que ainda não tenha sido corrigida, podemos ter acesso total ao sistema. No caso de falha em um servidor FTP, dependendo da sua gravidade, poderia nos levar a ter acesso direto ao shell do sistema.”

Buffer Overflow

O *Buffer Overflow* é uma área de memória temporária que recebeu dados além da sua capacidade de armazenamento. CICUNB: “Um *Buffer Overflow* é resultado do armazenamento em um *buffer* de uma quantidade maior de dados do que sua capacidade.”

BDJur
http://bdjur.stj.gov.br

Os atacantes utilizam a técnica de preencher o *Buffer* até que este “estoure”, em seguida o fluxo normal do processamento de informações é quebrado e o *Hacker* pode obter privilégios a mais do que tinha. A idéia é estourar o buffer e sobrescrever parte da pilha, mudando o valor das variáveis locais, valores dos parâmetros e/ou o endereço de retorno. Altera-se o endereço de retorno da função para que ele aponte para a área em que o código que se deseja executar, onde encontra-se armazenado o código malicioso. Pode-se assim executar código arbitrário com os privilégios do usuário que executa o programa vulnerável ARAUJO:63 “Suponhamos que eu esteja fazendo um programa em linguagem C .(poderia ser qualquer uma) e nele crio um buffer, um espaço na memória destinado a receber entrada de dados. Veja o exemplo a seguir:

```
#include <stdio.h>

#include <stdlib.h>

int main(int argc, char **argv){

char buffer[10];

strcpy(buffer, “testandostackoverflow”));

return 0;

}
```

Nesse pequeno programa, definimos o tamanho do buffer como 10 caracteres e copiamos para ele (através da função strcpy) um texto (string) contendo 21 caracteres. Como a função strcpy, ao contrário de strncpy, não faz a checagem do tamanho do espaço disponível, esse programa causará um estouro de buffer, fazendo com que você possa incluir código personalizado para ser executado pelo programa.”

BDJur
http://bdjur.stj.gov.br

Race Condition

Race condition é um termo que se refere a uma falha de segurança em sistemas que permite ao atacante elevar seus privilégios de acesso. Ocorre quando mais de um processo tenta acessar informações ao mesmo tento gerando alguns segundos de espera, nesse período o atacante pode executar uma rotina para elevar seu nível de acesso VIVAOLINUX: "O race condition acontece quando temos vários processos do sistema acessando e manipulando ao mesmo tempo a mesma informação de maneira concorrente e o resultado da execução depende da ordem particular em que o acesso ocorre.O race condition é muito interessante para invasores que querem elevar seu nível dentro de um sistema comprometido (obter uid=0(root))".Vamos ver um pequeno pedaço de código em C que ilustra um race condition:

```
if(access("/tmp/arquivo-info",R_OK)==0) {

   fd=open("/tmp/arquivo-info");

   process(fd);

   close(fd);

}
```

O código acima cria o arquivo temporário "arquivo-info" e depois abre ele. A vulnerabilidade em potencial ocorre entre as chamadas das funções access() e a chamada open().Se um atacante consegue manipular o conteúdo do "arquivo.info" entre as funções access() e open(), ele pode muito bem manipular qual vai ser a ação que o programa que utiliza esse arquivo vai realizar, isso e o que chamamos de "Race". O race condition não é um ataque trivial de ser realizado porque necessita de muitas tentativas até que o atacante consiga algum retorno efetivamente útil. Porém, se conseguir que o programa suid que utiliza esse arquivo no /tmp execute (access()) em sua instrução, sua chance de obter uid=0 será grande. O uso inapropriado de funções como access(), chown(), chgrp(), chmod(), mktemp(), tempnam(), tmpfile(), e tmpnam() são as principais causas de races conditions.

BDJur
http://bdjur.stj.gov.br

2.3.5 Burlando Proteções

A Próxima fase de um ataque *Hacker* ao sistema é burlar as proteções existentes. O principal objetivo do *Hacker* nesta etapa é elencar todas as proteções existentes no sistema de forma a evitar que estas possam rastrear seu comportamento. Basicamente existem 3 tipos principais de proteções na rede, Antivírus, Firewall e IDS.ARAUJO:90 "...temos que checar as proteções que o sistema-alvo possui e descobrir como burlar todas elas. Assim, passaremos despercebidos dentro do sistema. Vamos nos concentrar em como burlar três tipos de ferramentas: o antivírus, o firewall e o IDS."

Antivírus

Diferentemente do IDS e Firewall, que são mais utilizados em ambientes coorporativos, o antivírus é uma ferramenta existente em praticamente todos os sistemas sejam eles empresariais ou domésticos, mas muitas das tarefas realizadas pelos antivírus são comuns, como a análise seqüencial de caracteres. A maioria dos antivírus implementa a checagem de uma seqüência específica de caracteres existentes dentro de um arquivo. Um *Hacker* pode burlar esta proteção alterando a seqüência de caracteres. ARAUJO:90 " Atualmente, pela quantidade de vírus existente e pelo volume cada vez maior de arquivos a serem analisados, o antivírus tem que ter um processo rápido de identificação de infecção. Ele faz isso analisando uma seqüência de caracteres dentro dos arquivos: se encontrar alguma que esteja em seu banco de dados, ele identifica como vírus. Se modificarmos essa seqüência específica ou simplesmente realizarmos alguma alteração no texto que está dentro do executável (obviamente estando sempre realizando backups e testando para não correr o risco de corromper e perder o arquivo), o antivírus não mais detectará o software malicioso."

Firewall

Firewall é um dispositivo de segurança implementado para proteger toda uma rede interna de uma organização, ou as conexões internas de um sistema. Geralmente, o firewall é usado para bloquear tráfego externo deixando passar conexões internas para fora. ARAUJO:98 " Geralmente, o firewall é configurado para uma excelente proteção de fora para dentro, deixando passar, muitas vezes, apenas conexões a servidores WEB, de correio e algum tipo de serviço remoto que possua autenticação segura, como o SSH."

BDJur
http://bdjur.stj.gov.br

Existem várias formas de se burlar um Firewall, dependendo do tipo de acesso que se deseja realizar. Uma das maneiras mais utilizadas pelos *Hackers* é o *Spoofing* . Nessa técnica o atacante altera as configurações padrões de uma máquina fazendo que esta se passe por outra na rede. ARAUJO:102 " Spoofing é a arte de criar informações de rede falsas e utilizá-los para diversos propósitos: evitar ser capturado nos logs do sistema fazendo o que não devia, realizar scanneamentos estando totalmente ocultado ou ganhar acesso a máquinas que são protegidas por configurações de firewall. Um dos tipos de Spoofing, é o IP Spoofing. Exemplo: Uma máquina da rede interna só aceita comunicar-se com o endreço IP 192.168.0.1 e o seu é 192.168.0.110. Você não poderia mudar o seu endereço, isso criaria um conflito na rede. Mas você poderia utilizar o IP Spoofing, uma das técnicas mais usadas para personificar quem você não é. Para simplificar, pense da seguinte maneira: é como você chegar em algum local que te peçam um documento e você mostrar uma identidade falsa. Essa identidade não tem foto, somente um nome. A pessoa que está fazendo a segurança checa o nome, vê que está na sua lista e deixa entrar.Apesar de ser tecnicamente um pouco complexo, o conceito de spoofing é bem simples. Temos vários tipos: ARP Spoofing (spoofing de endereços MAC de rede através do protocolo ARP), DNS Spoofing e, claro, IP Spoofing."

Existem dois tipos de IP Spoofing, cego e não-cego, no primeiro caso o atacante não consegue ver a resposta do alvo. No segundo caso, o não-cego, o *Hacker* obtém a resposta do alvo. ARAUJO:102 "...Geralmente, quando realizamos IP Spoofing, modificamos o pacote a ser enviado, colocando outro endereço que não seja o nosso. Esse pacote irá até o seu destino e será processado por ele de alguma maneira, seja enviando uma resposta ou simplesmente recusando-o. Agora como faremos para ver essa resposta, já que o endereço que está na informação enviada não é o nosso ? A resposta é simples: se estamos em uma rede local, podemos sniffar (farejar a rede), como visto no capítulo sobre sniffers. Isso seria o spoofing não-cego, pois você pode ver a resposta do alvo, mesmo que ela seja endereçada a um endereço falso e inexistente."

Um dos programas mais usados para o IP *Spoofing* é o *Sterm*, este programa é um tipo de cliente Telnet que forja o endreço IP de um sistema. ARAUJO:104 "consegue realizar um *Spoof* full-duplex (ele consegue receber os dados também, sem você precisar ficar utilizando um sniffer à parte para fazer isso). Quando realizar uma conexão, será como se tivesse em uma sessão de Telnet comum, o que facilita muito o trabalho de entrar de modo oculto em algum local.Para conseguir essa façanha, o sterm se vale do "ARP poisoning/spoofing". O pedido ARP está essencialmente perguntando: "Qual o endereço de hardware correspondente ao endereço IP que tenho aqui ?. Normalmente, somente o host com o IP correspondente envia uma resposta ARP e o resto dos computadores ignora o pedido ARP.

BDJur
http://bdjur.stj.gov.br

Ele envenena então o cachê ARP dos computadores que mantêm a lista dos endereços MAC e seus respectivos endereços IPs, respondendo com o endereço IP que você quiser.

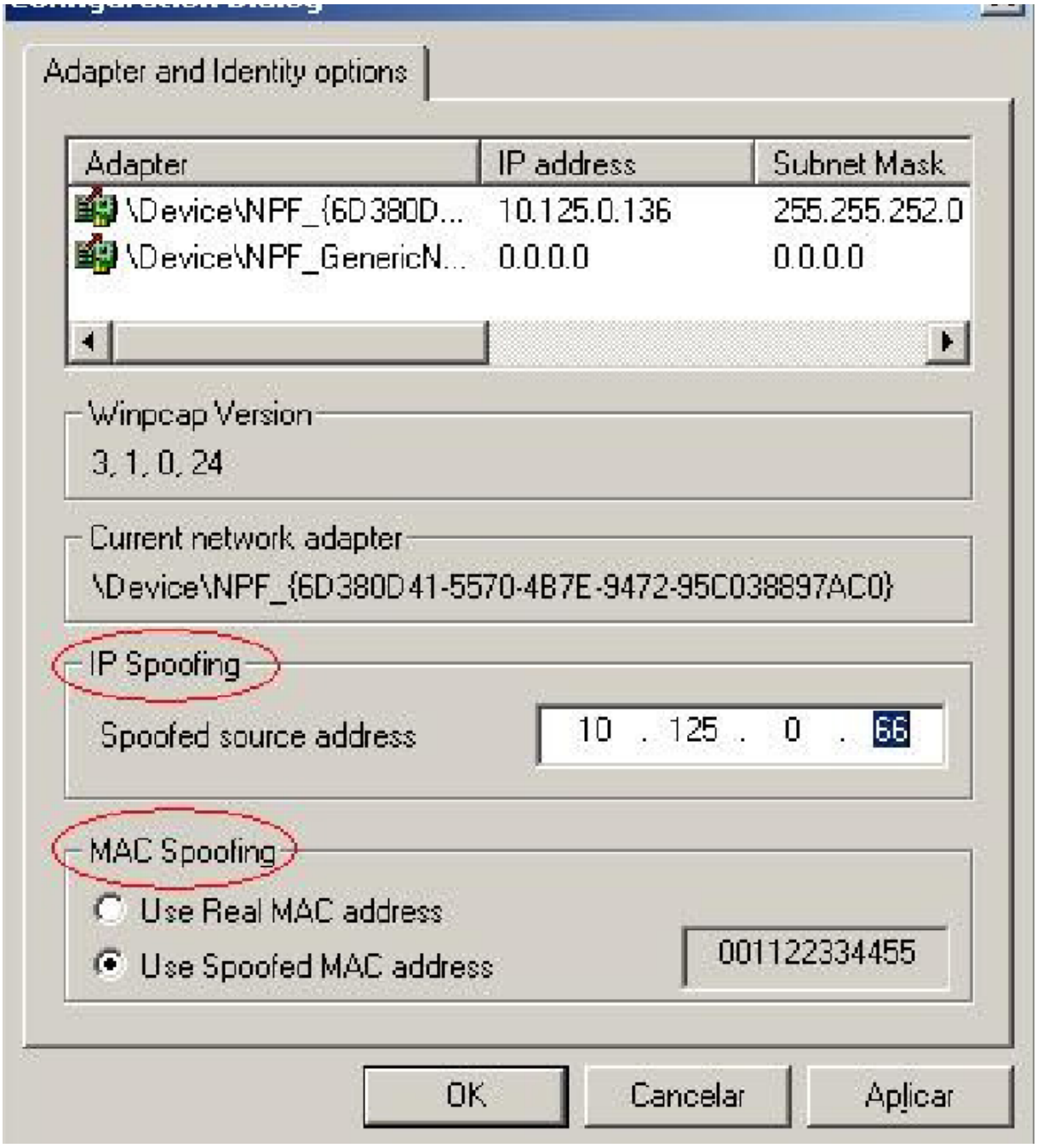

Figura 2.3.5 – *Spoofing* utilizando o programa Sterm.

Após decidir o adaptador de rede, o endereço IP falso e, ainda, ter a possibilidade de escolher se vai realizar um MAC real ou 'spoofado' (Mesmo sendo o MAC falso, o programa consegue receber as informações de volta ? Por Quê ? Ele cria entradas duplas no ARP.), já estamos

BDJur
http://bdjur.stj.gov.br

prontos para nos conectarmos onde for. A opção a seguir aparecerá para escrevermos o endereço IP e a porta que iremos nos conectar.

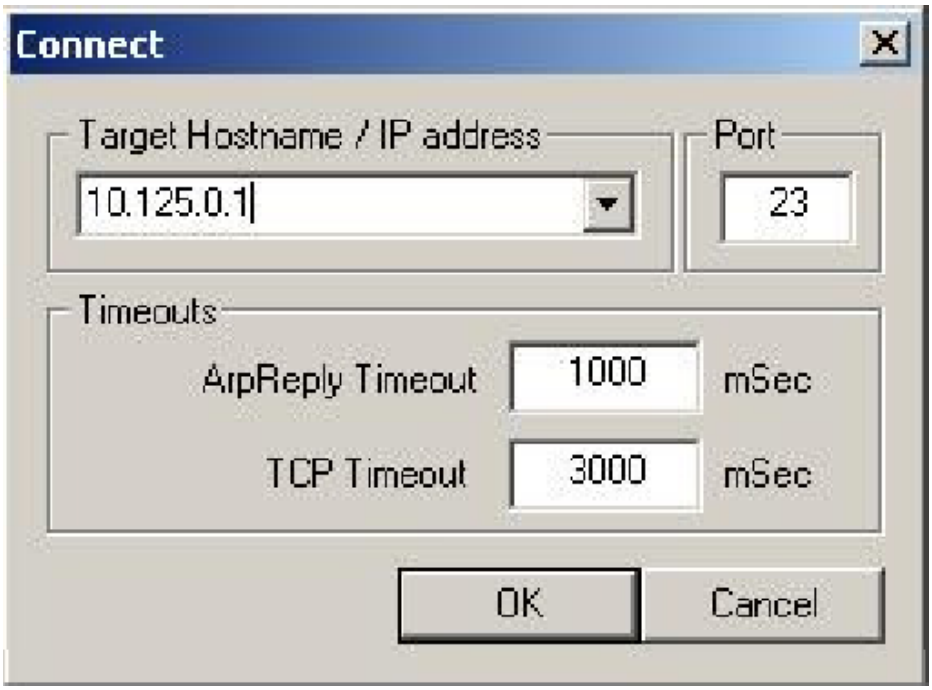

Figura 2.3.5.1 – Configurando IP e porta no Sterm para Spoofing.

Clicando em Ok estaremos realizando um spoofing de endereço IP, estando anônimo na conexão e, como podemos ver, pareceremos estar utilizando uma sessão de Telnet comum, como qualquer outra. Deixemos as opções ARPReply *Timeout* e *TCP Timeout* nos números padrões. Se a conexão estiver um pouco lenta, diminuí-los um pouco até estarmos satisfeitos. O resultado, observamos na seqüência:"

BDJur
http://bdjur.stj.gov.br

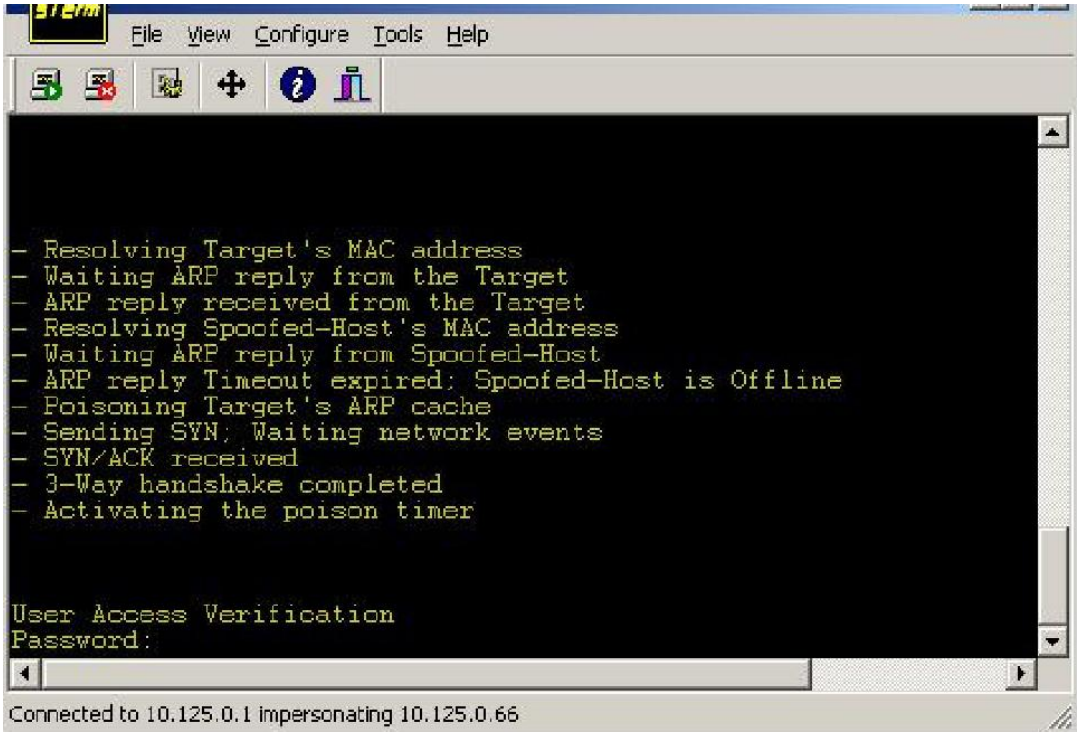

Figura 2.3.5.2 – Resultado do Spoofing usando Sterm.

Observe a barra inferior do programa: Conectado a 10.125.0.1 impersonando 10.125.0.66. Significa que o spoofing foi um sucesso. Outra linha interessante é o "*Poisoning Target´s ARP Cache"*, que significa: Envenenando o cachê ARP do alvo. O único problema do *STERM* é que, apesar de fantástico, ele só consegue realizar *spoofing* não-cego.

IDS

O IDS é um Sistema de Detecção de Intrusão, sua função é detectar possíveis invasões na rede. LAUFER: "analogamente a um sistema do mesmo nome empregado na segurança domiciliar, é composto por sensores capazes de disparar um alarme caso algum evento determinado ou não esperado venha a acontecer. Detecção de intrusão é uma tentativa de monitorar estações ou fluxos de rede com o intuito de descobrir ações de intrusos. Mais especificamente, um SDI tenta detectar ataques ou usos impróprios e alerta o responsável pela rede do acontecimento. O funcionamento é análogo ao de um sistema de detecção de ladrões, usado em casas para se proteger de eventuais incidentes. O sistema domiciliar inicialmente precisa ser configurado e ter especificado o que monitorar (janelas, portas, movimento) e para quem alertar ou chamar em caso de uma invasão (polícia, donos da casa). No sistema computacional, também precisamos determinar se queremos monitorar fluxos de rede,

BDJur
http://bdjur.stj.gov.br

processos internos de uma estação ou servidor, ou ainda um sistema de arquivos, por exemplo. E devemos deixar claro para quem enviar os alarmes ou relatórios e como estes devem ser enviados, tendo como alternativas o e-mail, pager, ou ainda um pacote SNMP. Teoricamente, esse tipo de sistema seria somente passivo, observando pacotes na rede ou processos em uma estação de trabalho e alertando os responsáveis. Porém, alguns sistemas possuem a habilidade de reagir às invasões, deixando de ser um sistema exclusivamente de detecção e pode ser definido como um sistema de reação a intrusão. Exemplos de reação podem ser um fechamento de conexão, um bloqueio no firewall, execução de algum arquivo, ou ainda a desabilitação de uma conta".

Para Burlar um IDS a técnica mais utilizada pelos invasores é enviar pacotes de forma que a assinatura do IDS não coincida.ARAUJO:119 " A assinatura é geralmente considerada uma condição ou string(pedaço de texto) que está presente nos pacotes que atravessam a rede. Na maioria das vezes, funciona assim: o IDS procura uma assinatura (como, por exemplo, a string */CGI-bin/phf*) no tráfego da rede e, se encontrar, o sistema de detecção irá anunciar como se fosse um ataque" . Uma forma muito comum é alterar o método GET por HEAD, a maioria dos sistemas de IDS usam filtros para o GET e não para o HEAD. ARAUJO:119: "GET /CGI-bin/some.cgi O truque aqui é usar o HEAD... HEAD /CGI-bin/some.cgi" . Outra técnica bastante utilizada para burlar os IDSs é codificar o cabeçalho da URL em caracteres hexadecimais. Os endereços de URL podem ser escritos na notação %xx, onde xx é o valor em hexadecimal do caractere.O sistema IDS não conseguirá identificar um ataque codificado em hexadecimal uma vez que a assinatura CGI-bin não corresponde a string %xx. Outra forma de burlar as assinaturas é utilizar barras duplas ou triplas na URL. Exemplo: /teste/índex.php ficaria //teste//índex.php ou ///teste///índex.php.

2.3.6 Engenharia Social

Engenharia Social é uma técnica de sondagem, espionagem utilizada pelos *Hackers*. É geralmente utilizada quando as técnicas informatizadas não são suficientes para a execução de um ataque. Trata-se de um componente humano, o atacante, geralmente uma pessoa com bom poder de comunicação, irá tentar obter informações privilegiadas e sigilosas dos funcionários da empresa através da persuasão. A engenharia social, de maneira simples, caracteriza-se por explorar essa fragilidade. Em outras palavras, consiste na habilidade de obter informações ou acesso indevido a determinado ambiente ou sistema, utilizando técnicas de

BDJur
http://bdjur.stj.gov.br

persuasão. Podemos perceber que um ataque muita das vezes mobiliza vários *Hackers* e que a interdisciplinaridade dos atacantes é requerida quando se pretende realizar uma engenharia social, o nível cultural do engenheiro social deve ser elevado de forma a obter a informação desejada. ARAUJO:125 " Os engenheiros sociais são pessoa cultas, de um papo agradável e que conseguem fazer com que você caia em suas armadilhas. Utilizando meios digitais, telefônicos e até pessoalmente, observam e estudam você sem que sejam percebidos. E isso não é algo novo que surgiu com a informática, há décadas esses engenheiros vêm agindo. Por aqui, normalmente conhecemos essas pessoas por estelionatários."

Os engenheiros sociais agem basicamente de três formas, a saber:

- Por e-mail ou carta:

  Por esse meio o atacante solicita informações ou documentos se fazendo passar por uma pessoa importante ou integrante de algum projeto ou trabalho. Geralmente utilizado por não expor muito o atacante. Essa técnica é utilizada na maioria das vezes com a técnica de seqüestro de e-mail, onde o atacante já roubou o e-mail de uma pessoa da equipe da empresa atacada.

- Pessoalmente:

  Nesse ataque a pessoa se faz passar por alguém importante, muito bem trajado, com notebook e maleta o atacante tenta adentrar na empresa e em áreas restritas apenas ao pessoal autorizado.Outra maneira de se obter informações pessoalmente na empresa é fazer-se passar por um faxineiro e revirar o lixo em busca de informações sigilosas.

- Por telefone:

  Muitas vezes o engenheiro procura aflorar os sentimentos do atacado via telefone. Tenta se passar por um cliente ou usuário e finge precisar de ajuda, ao convencer o ouvinte solicita alguma informação privilegiada ou sigilosa como senhas, códigos, etc...

  Alguns casos curiosos os engenheiros não precisam utilizar de técnicas de persuasão, bastando ter apenas o acesso físico ao local ARAUJO:126 "...Vestiu-se com um belo terno e se apresentou à segurança como um investidor internacional da empresa, citando nomes de várias pessoas que trabalhavam lá dentro. Claro, ele pesquisou as pessoas que estariam de férias na ocasião e as citou. Após ter a entrada liberada, ele dirigiu-se para o

BDJur
http://bdjur.stj.gov.br

elevador mais movimentado da empresa. Subiu com ele para o último andar. Depois de todos deixarem o elevador, Daniel tirou cuidadosamente um CD de seu bolso e colocou no piso do elevador. Na capa do CD estava escrito “Fotos comprometedoras”.Despistadamente, então, ele deixou o prédio e foi checar o seu notebook com conexão à rádio. Meia hora depois, ele conseguiu um acesso para dentro da empresa. Isso porque alguém não agüentou de curiosidade e abriu o conteúdo do CD no seu computador da empresa”.

Capitulo 3 – Processo cognitivo

3.1 A formação do “Saber humano”

Para entendermos como o processo cognitivo se forma devemos buscar na história da humanidade o entendimento de como a *epistémê* moderna define o saber humano.(FOUCAULT,1999, p.479): “o campo da epistémê moderna não se ordena conforme o ideal de uma matematização perfeita e não desenrola, a partir da pureza formal, uma longa seqüência de conhecimentos descendentes, cada vez mais carregados de empiricidade. Antes, deve-se representar o domínio da epistémê moderna com um espaço volumoso e aberto segundo três dimensões. Numa delas, situar-se-iam as ciências matemáticas e físicas, para as quais a ordem é sempre um encadeamento dedutivo e linear de proposições evidentes ou verificadas;haveria, em outra dimensão, ciências (como as da linguagem, da vida, da produção e da distribuição das riquezas) que procedem ao estabelecimento de relações entre elementos descontínuos mas análogos, de sorte que elas pudessem estabelecer entre eles relações causais e constantes de estrutura. Essas duas primeiras dimensões definem entre si um plano comum: aquele que pode aparecer, conforme o sentido em que é percorrido, como campo de aplicação das matemáticas a essas ciências empíricas, ou domínio do matematizável na lingüística, na biologia e na economia. Quanto à terceira dimensão, seria a da reflexão filosófica, que se desenvolve como pensamento do mesmo; com a dimensão da lingüística, da biologia e da economia, ela delineia um plano comum: lá podem aparecer, e efetivamente apareceram, as diversas filosofias da vida... mas, lá também apareceram, se interrogar-se de um ponto de vista radicalmente filosófico o fundamento dessas empiricidades..., a dimensão filosófica define como a das disciplinas matemáticas um plano comum: o da formalização do pensamento.”

BDJur
http://bdjur.stj.gov.br

3.2 Motivação

Ao falarmos de motivação humana devemos considerar dentro do exposto sobre as três dimensões da formação do saber humano como elas influenciam uma determinada conduta ou comportamento. Nossa perspectiva de análise é o comportamento *hacker*, e como tal verificamos que a criatividade e a intuição são as características principais desse fenômeno. Abordemos o conceito de criatividade: O termo origina-se do século XVIII, do romantismo ARTECRIATIVA: "O conceito de criatividade, remontando à Antigüidade, estava também associado à loucura, pela sua natureza de irracionalidade, principalmente relacionado ao gênio na criação artística. A concepção de que o artista cria em estado de loucura, real ou potencial, permanece ao longo do tempo. Durante o século XIX a ligação entre o gênio e a loucura torna-se foco de estudo da Psicologia, que estabelecia uma estreita associação entre a criação artística e o estado psicótico.Uma outra concepção que encontra sua origem no pensamento do século XVIII, consiste na de associar a capacidade criativa à imaginação. Esta seria a livre associação de idéias obtida por inspiração e dom, que favorecia os "gênios", indivíduos de mente criativa,capazes de criar numa condição diferenciada dos demais indivíduos."

Dentro dessa livre associação de idéias que culmina na imaginação percebemos uma forte tendência à utilização da relativização "foulcautiana". Uma primeira definição de imaginação, restringida à sua referencialidade, pode dizer respeito à capacidade mental para relacionar, criar, inventar ou construir imagens.O termo é derivado do latim imaginatio, que por sua vez substitui o grego phantasía. Aristóteles, em De Anima (428a 1-4), deu-nos uma primeira reflexão teórica sobre o conceito de imaginação (phantasía) que se refere apenas ao processo mental através do qual concebemos uma imagem (phantasma). A imaginação é uma forma de representação do que sentimos não existir no nosso mundo próximo. Esta origem grega do conceito mantém-se em alemão (Phantasie), sendo esta a forma que os primeiros grandes teóricos do inconsciente, Freud e Jung, sempre utilizaram.

No que se refere à motivação de um comportamento *hacker*, por exemplo, invasão de um sistema contábil, devemos considerar que o atacante inicialmente irá utilizar-se da primeira dimensão "faucoultiana", a saber, a matematização ou classificação. FOUCAULT,1999,p. 479) "...as ciências matemáticas e físicas, para as quais a ordem é sempre um encadeamento dedutivo e linear de proposições evidentes ou verificadas". Isso porque o *Hacker* primeiramente deverá ter um

BDJur
http://bdjur.stj.gov.br

conhecimento prévio sobre o sistema contábil, ele deverá ter uma idéia ou classificada de como é um sistema contábil e quais as suas regras de negócio e conseqüentes elementos de segurança implementados. Mas o que motivaria o ataque estaria relacionado ao desejo do *Hacker* por aguçar, aumentar cada vez mais a sua capacidade criativa e imaginativa em contraste ao apreendido, classificado pela matematização. Essa motivação aproxima-se da relativização de Foucault : (FOUCAULT,1999,p. 479) " ... ciências (como as da linguagem, da vida, da produção e da distribuição das riquezas) que procedem ao estabelecimento de relações entre elementos descontínuos mas análogos, de sorte que elas pudessem estabelecer entre eles relações causais e constantes de estrutura". A insatisfação do atacante está não no fato de se conseguir ou não atacar um sistema, ou de busca de desafio como muitos imaginam, mas está mais relacionada ao processo cognitivo como um todo.Ter a liberdade de saber como as coisas funcionam é o principal motivo de fazer o que fazem. Uma frase muito comum no mundo *hacker* define a conduta geral de um White Hat: "Hack to learn, not learn to hack" (em tradução livre, "Invadir para aprender, e não aprender para invadir").

3.3 Elementos Observáveis

Considerando que já mapeamos o processo cognitivo, o processo criativo e a motivação dos atacantes podemos intuir alguns elementos dentro do comportamento *Hacker* que podem contribuir para a construção de uma solução que simule uma realidade de sistema de informação que possibilite aos gestores de segurança em redes obterem dados importantes do perfil dos seus atacantes. Os elementos serão observados e relacionados ao processo criativo do atacante enquanto negação de uma realidade. Segundo VYGOTSKY (1982,p.31-32), a imaginação criadora é motivada pela capacidade de fantasiar a realidade: "A imaginação criadora é resultante da capacidade de fantasiar situações. O indivíduo irá criar segundo a sua capacidade de imaginar e fantasiar com base numa série de fatores, entre eles, a experiência acumulada, enquanto um produto de sua época e seu ambiente." Nesse ponto criamos o sistema simulado com simulações intercaladas, ora documentos da área financeira, ora da área administrativa, por exemplo. Obteremos assim dados referentes à realidade que o atacante deseja fantasiar. O administrador poderá implementar um banco de dados estatístico classificando cada invasão de acordo com as principais motivações. Uma mudança nos valores de salários em uma planilha simulada do setor de recursos humanos,

BDJur
http://bdjur.stj.gov.br

por exemplo, pode ser classificada como um ataque motivado a alterar uma realidade de desigualdade social. Cada ataque sucessivo mas com motivação diferente deve ser um novo elemento observável.

Capitulo 4 – Utilização de *Honeypot*

4.1 Conceito de *Honeypot*

Inicialmente para entendermos o conceito de "*Honeypot*" devemos elucidar a sua origem. Os *honeypots* surgiram como continuidade ou desmembramento dos sistemas de detecção de intrusão IDS (*Intrusion Detection System*), o IDS é uma ferramenta que monitora as atividades dos acessos na rede alertando os administradores quando um acesso indevido é identificado. Os alertas podem ser classificados como falso-positivo ou falso-negativo: *ASSUNÇÃO(2009)*, 17: "a prefeitura de Salvador instalou câmeras de segurança nas principais avenidas durante o carnaval. O objetivo seria detectar furtos e pequenos incidentes com os turistas. Mas o trafego de pessoas é tão grande, que podem acontecer dois problemas:

- Primeiro, o falso-positivo – Um folião se anima e começa a flertar com uma moça, mas quem esta analisando os dados das câmeras acredita ser um assalto e toma as medidas necessárias.
- Segundo, o falso-negativo – Um ladrão passa perto de uma vitima e delicadamente furta o celular de dentro do bolso dela sem que a pessoa e as câmeras percebam o delito, por causa do movimento excessivo."

Honeypot é uma armadilha feita para detectar, pegar, desviar ou em algum modo contrariar as tentativas de conexão não autorizadas.Trata-se de uma simulação de ambiente em que o administrador pode monitorar as atividades de um invasor : *ASSUNÇÃO(2009)*,18: "é como se você comprasse uma casa e a mobiliasse parcialmente, com alguns poucos moveis. A casa teria normalmente duas portas e duas janelas que servem como entrada e saída (o que seriam os serviços no *honeypot* de computador). Acontece que você não disse a ninguém que adquiriu o imóvel . Então, a não ser você, qualquer pessoa que entrar ou sair da casa é um invasor, com cem por cento de certeza."

BDJur
http://bdjur.stj.gov.br

4.2 Implementação de um *Honeypot*

O primeiro passo para implementar um *Honeypot* é definir quais ambientes e serviços serão simulados para os invasores de forma a atraí-los. *ASSUNÇÃO(2009)*,30: “É importante que estes serviços sejam atrativos aos atacantes. Podem ser programas que funcionem como servidores de correio ou de transferência de arquivos”. É importante fornecer serviços com funcionalidade real, onde toda a interface de sistema operacional, banco de dados, serviços web estejam integrados e padronizados.

Existem basicamente dois tipos de *Honeypots*:

4.2.1 Honeypot de Produção

São os sistemas simulados onde o foco do administrador de segurança é detectar uma invasão sem se preocupar com o comportamento do *Hacker*. *ASSUNÇÃO(2009)*,31: “Sua intenção é praticamente apenas detectar intrusos na rede e tomar as providências contra esses invasores o mais rápido possível. É o que normalmente seria utilizado em alguma empresa ou instituição que deseja proteger a sua rede.”.No caso do *honeypot* de produção deve se implementar uma simulação com requisitos de segurança específicos para não comprometer os ativos de rede.O principal objetivo de um *honeypot* de produção é identificar o ataque e desviá-lo ou contê-lo o mais rápido. Outro ponto importante é o fato de o atacante descobrir ou não a existência do *Honeypot*. No caso do *honeypot* de produção o atacante pode conhecer sobre o ambiente simulado uma vez que seu ataque já foi contingenciado.

4.2.2 Honeypot de Pesquisa

Neste tipo de simulação o administrador de segurança está interessado em saber sobre o comportamento do invasor. Nessa implementação as funcionalidades de detecção de intrusão não necessitam estar habilitadas. O ambiente deve ser

BDJur
http://bdjur.stj.gov.br

cuidadosamente montado para que o atacante não perceba que está em um sistema simulado *ASSUNÇÃO(2009)*,30: “Um *honeypot* de pesquisa não tem como objetivo primário ser utilizado como uma ferramenta de IDS. O que ele pretende é realmente ser atacado várias vezes e, com isso, estudar todos os detalhes de cada ataque. Cada arquivo que o invasor acessar, cada senha que ele digitar, cada comando, absolutamente tudo será salvo e estudado.”

Os *Honeypots* de pesquisa serão utilizados para se estudar os ataques realizados pelo *hacker*, assim é primordial que o ambiente possua uma grande interatividade com serviços. *ASSUNÇÃO(2009)*,30: “...devem ser utilizados apenas com serviços de alta interação.”

4.2.3 Localização do *Honeypot*

Idealmente o *Honeypot* deverá ser localizado entre as conexões externas e o Primeiro “Firewall”. Isso porque nossa implementação será um *Honeypot* de Pesquisa e quanto mais exposto e acessível pelos atacantes melhor. Os riscos inerentes a esta exposição deverão ser analisados e aceitos pela equipe de segurança. *ASSUNÇÃO(2009)*,28: “ Neste caso o *honeypot* vai ficar propositalmente exposto ao máximo sem ter nenhum tipo de proteção. É uma situação em que provavelmente o invasor conseguirá causar mais danos, mas justamente por isso, é o mais interessante do ponto de vista de capturar ações maliciosas, que é o objetivo de um *honeypot* de pesquisa”

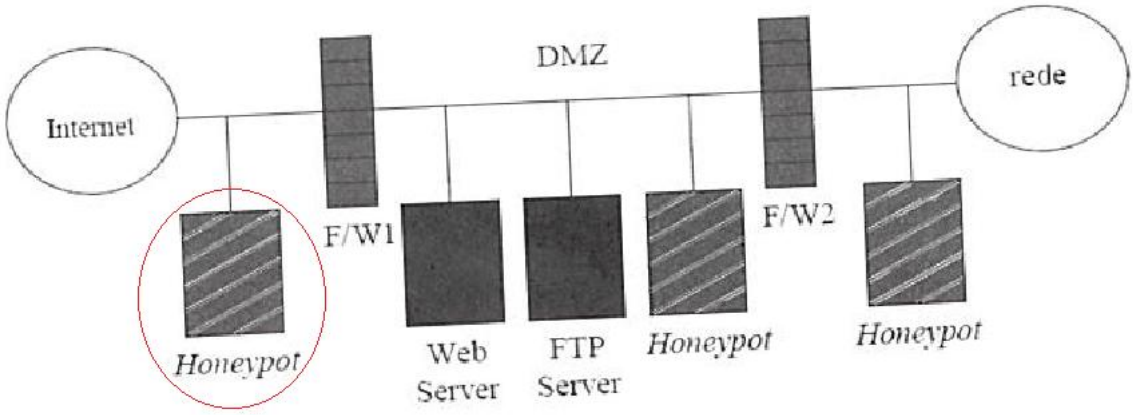

Figura 4.2.3 – Localização do Hoenypot na rede.

BDJur
http://bdjur.stj.gov.br

4.2.4 Honeyd

Para implementarmos o *honeypot* sugerimos o uso do software honeyd em virtude de sua flexibilidade de configuração. De acordo com HONEYDREF, Através de scripts, o honeyd é capaz de simular diversos sistemas operacionais e são suportados os protocolos UDP, TCP e ICMP . O desenvolvimento do honeyd trouxe novos conceitos para as tecnologias associadas a *Honeypots* como por exemplo ele não responde apenas a ataques direcionados ao próprio IP pois pode assumir diversas identidades. É conceitualmente a aplicação de *Honeypots* para toda a rede. Além disso, pode simular diversos Sistemas Operacionais ao mesmo tempo. Por fim outro novo conceito é a capacidade do honeyd em emular além das aplicações a pilha TCP, fazendo com que estes serviços emulados se comportem como verdadeiros Sistemas Operacionais. Funcionamento Pela incapacidade do honeyd em direcionar para si todos os ataques ele deve identificar os endereços IP que não estão ativos na rede. Ele realiza isso em duas situações de configurações diferentes de ambiente de rede. A primeira corresponde a situação onde não existem sistemas ativos e sim apenas o honeyd. Para tanto, ele utiliza o método blackholing. O funcionamento é análogo ao buraco negro, pois como sabemos que não existe serviço ativo, então certamente é um ataque e por conseqüência direcionamos todo o tráfego para o *Honeypot*. A segunda situação corresponde a uma topologia onde temos além do *Honeypot*, um ambiente de produção real. Nesse ambiente o honeyd utiliza uma forma mais complexa de direcionar este tráfego, através de outro programa ARPD utilizando o método de ARP spoofing ou ARP proxy. Esta ferramenta atuando juntamente com o honeyd atende as requisições ARP através da monitoração dos endereços IP que não estão ativos. Agora com as requisições ARP sendo todas atendidas, ou seja, mesmo quando um endereço IP não existente é atacado o Honeyd assume a identidade de vítima e interage com o atacante (18). Após essa conexão, a porta selecionada pelo atacante é identificada e inicia-se a interação. De acordo com as diversas possibilidades de configuração, a porta requisitada pode ou não estar sendo atendida por algum serviço emulado. Se estiver, o atacante pode receber como resposta, por exemplo, uma seqüência de “login” ou então uma emulação de um servidor WEB, caso contrário pode-se simplesmente bloquear a porta informando esta situação ou simplesmente não haver qualquer retorno. A possibilidade de emulação de diversos sistemas operacionais

BDJur
http://bdjur.stj.gov.br

através da criação de hosts virtuais permite a criação de topologia de redes inteiras, formadas por roteadores, servidores, clientes todos com características específicas.Dentre os arquivos de configuração do honeyd, está o nmap.prints, que contém a mesma tabela de assinaturas que o Nmap, uma das ferramentas mais comumente usadas para remotamente identificar o tipo de sistema operacional, utilizada para comparar o padrão de resposta, permitindo aos *Honeypots* virtuais responder exatamente como o sistema operacional que ele emula, quando testado pelo Nmap.Outro arquivo, usualmente nomeado como honeyd.conf contém os templates que definem as características dos *Honeypots*. Existem inúmeras possibilidades de criação e cabe ao usuário definir ao seu critério, dando a Baseado nas práticas de Software Livre, todo o código do honeyd é disponibilizado o que nos permite customizar para fins específicos.

4.3 Instalação e Configuração do *Honeypot* (*honeyd*)

Para hospedar nosso *honeypot* usaremos uma máquina rodando Linux e usaremos os procedimentos abaixo para instalar o “Honeyd” - HONEYDREF

Acessar o site do Honeyd e baixar os sources mais recentes: http://www.citi.umich.edu/u/provos/honeyd/honeyd-1.5b.tar.gz

O Honeyd precisa de algumas bibliotecas para ser compilado com sucesso. É necessário o Python, o Perl, a libevent (http://www.monkey.org/~provos/libevent/), a libdnet (http://libdnet.sourceforge.net/) e a libpcap (http://www.tcpdump.org/). A instalação dessas dependências é extremamente simples (em quase todas se resumindo a ./configure, make, make install).

Instalar o arpd (http://www.citi.umich.edu/u/provos/honeyd/arpd-0.2.tar.gz)

Iremos configurar o *Honeypot* com um servidor Linux de kernel 2.4 simulado disponibilizando um serviço de correio eletrônico usando os comandos abaixo:

```
create linux
set linux personality "Linux 2.4.16 - 2.4.18"
set linux default tcp action reset
set linux default udp action reset
set linux uptime 3284460
```


BDJur
http://bdjur.stj.gov.br

```
add linux tcp port 110 "sh scripts/pop3.sh"
add linux tcp port 25 "sh scripts/smtp.sh"
add linux tcp port 22 "sh scripts/test.sh $ipsrc $dport"
bind 192.168.0.2 linux
```

Para emular os serviços de correio eletrônico utilizaremos os seguintes scripts:

- pop3.sh: emula um serviço POP3 na porta 110
- smtp.sh: emula um serviço de SMTP na porta 25
- teste.sh $ipsrc $dport: emula o SSH, logando o IP de origem (de quem se conectou ao script) e em qual porta.

Para a verificação de quais sistemas operacionais podemos emular usando o Honeyd, é só executar o seguinte comando:

```
#  grep "^Fingerprint" nmap.prints | less
```

Após as configurações do Servidor de correio eletrônico simulado faz-se necessário redirecionar o tráfego de endereços não utilizados na rede para o *honeypot*.Para isso usaremos o ARPD para fazer com que o *honeypot* responda na rede para qualquer endereço que não esteja sendo utilizado(não utilizar DHCP na rede em que o *honeypot* estiver respondendo):

```
arpd 192.168.0.0/24
```

Por fim, após estas configurações, podemos iniciar nosso *honeypot* que irá simular um servidor de correio eletrônico utilizando o seguinte comando:

```
#  honeyd -p nmap.prints -f /etc/honeyd.conf 192.168.0.0/24
```

4.4 Redesenhando um *Honeypot* de acordo com o comportamento *Hacker*

Neste ponto utilizaremos a terceira dimensão foulcautiana como elemento de estudo do comportamento *hacker*, a saber a capacidade filosófica e reflexiva do ser humano, para estimular a completa compreensão do Administrador de segurança sobre os invasores e seus ataques, seus comportamentos enquanto invasor. Segundo Foucault, (FOUCAULT,1999, p.479), a terceira dimensão corresponde ao processo reflexivo e filosófico que temos sobre nossas experiências cognitivas.De acordo com os elementos observados pelo *Honeypot* redirecionamos o ataque para uma nova simulação em que desta vez o atacante não irá se deparar com uma realidade a ser fantasiada, a ser explorada de forma criativa, mas com uma realidade que ele já experimentou e que o faça não repetir o mesmo ataque utilizando a terceira dimensão foulcautiana do pensamento. Essa reflexão sobre as experiências vividas pelo invasor no ambiente simulado irá coibir novos ataques por inibir a motivação. O administrador utilizando-se dos elementos observáveis sobre o comportamento *hacker* poderá coibir o impulso criativo, motivador do atacante fornecendo uma nova simulação já vivenciada após algumas invasões. A idéia é intercalar as realidades, a cada 5 ou 10 simulações, repetir uma realidade afim de que o atacante reflita sobre seu potencial criativo.Após um trabalho exaustivo de invadir o sistema algumas vezes, e ao perceber que seus ataques não surtem mais efeitos no ambiente o atacante refletirá sobre seu comportamento e técnicas utilizadas e não irá mais atacar o sistema.

BDJur
http://bdjur.stj.gov.br

Conclusão

A utilização de técnicas de segurança em redes valendo-se sempre de padrões, normas e principalmente de elementos de monitoração de redes, na maioria das vezes, é modelada numa visão técnica e monodisciplinar, negligenciando a vertente psíquica envolvida nos incidentes de segurança. Devido ao alto custo de se estudar de forma efetiva o comportamentos dos *Hackers* as equipes de segurança da informação preferem investir os recursos e o tempo em medidas meramente técnicas e proibitivas que não fornecem informações sobre o comportamento dos atacantes.O trabalho aqui apresentado procurou disponibilizar uma solução em segurança da informação que pudesse fornecer informações não apenas sobre a possibilidade de simular uma realidade afim de monitorar acessos indevidos a rede, mas sobre o comportamento dos invasores no que diz respeito ao seu perfil intelectual e motivacional, a saber uma pessoa que busca estimular seu potencial criativo. A interdisciplinaridade aqui apresentada foi de vital importância para se traçar uma estratégia de estimulo ao processo reflexivo utilizando uma das técnicas mais modernas em segurança da informação. É Importante também salientar que este trabalho vem complementar a fraca bibliografia existente hoje no mundo acadêmico e mercadológico no que concerne à utilização dos Honeypots. Ao contrário do que possa parecer, a técnica de responder aos ataques e acessos maliciosos estimulando a reflexão dos invasores sobre seu comportamento não representa uma invasão da intimidade na medida em que apenas sugere novas variáveis ao invasor, sem coibir fisicamente ou repreensivamente qualquer atitude. Nossa solução fornece uma nova abordagem para os administradores de segurança da informação por tratar as invasões como iniciativas criadoras e não como ameaça. Ficamos aqui desejosos de que possam existir mais realidades simuladas que possam não apenas redirecionar os ataques a fim de preservar os ativos das organizações, mas que possibilitem o estudo do comportamento invasor como um todo.

BDJur
http://bdjur.stj.gov.br

Objetivo 1: Mostrar as vantagens da utilização de Honeypot como técnica de segurança.

No sub-capitulo 4.1 mostramos que o Honeypot permite além de detectar e documentar as tentativas de invasão ele permite redirecionar estes ataques para um ambiente que não seja o de produção. No sub-capítulo 4.2.4 explanamos que a utilização do Honeyd permite simular vários sistemas operacionais e protocolos, o que é uma grande vantagem para o administrador na medida em que ele dispõe de várias opções de simulação de ambiente para atrair diversos tipos de invasores.

Objetivo 2 - Identificar os principais ataques em redes e o comportamento *Hacker*.

Nos sub-capítulos 2.1 e 2.2 identificamos o comportamento *hacker* como uma atitude que busca explorar o potencial criativo.Conforme explanado diferentemente de um técnico acadêmico os *Hackers* utilizam-se mais da intuição do que de normas e procedimentos. No que se refere aos principais ataques em redes elencamos no sub-capitulo 2.3 vários destas atividades tais como *footprint*, varreduras e enumeração.

Objetivo 3 - Apresentar como o processo cognitivo pode oferecer elementos de mudança comportamental de *Hackers*.

Para conseguirmos este objetivo definimos o processo cognitivo em três dimensões conforme o sub-capitulo 3.1 e mostramos que a terceira dimensão “foucaultiana” em pode mudar o comportamento *hacker* ao ser implementada em um honeypot de simulações sucessivas com repetições intercaladas, definido no sub-capítlulo 4.4.

Como a utilização de “*Honeypot*” cognitivo pode contribuir para entender e controlar o comportamento *hacker* na segurança de redes.

O entendimento e o controle do comportamento *hacker* pelos administradores de segurança pode ser adquirido com a utilização das simulações possíveis de se implementar através do “honeyd” coletando informações sobre o atacante conforme descrito nos sub-capítulos 4.3 e 4.4.

BDJur
http://bdjur.stj.gov.br

REFERENCIAL BIBLIOGRÁFICO

CAPITULO I

NORTHCUTT- *Winters,scott,northcutt,Stephen.Frederick,Karen.Zeltser,Lenny.Ritchey,Ronald W.- Desvendando Segurança de Redes . Ed. Campos . São Paulo - 2002*

IGDUCA - *http://www.igeduca.com.br/artigos/nunca-e-tarde-para-aprender/o-que-sao-roteadores.html*

PROXY - *http://proxy.furg.br/proxy/*

IDSRNP - *http://www.rnp.br/newsgen/9909/ids.html#ng-o*

DMZREF - *http://jeancarloscunha.wordpress.com/2008/11/14/o-que-e-dmzconceito/*

CAPITULO II

MICHAELIS – *Dicionário on-line: http://michaelis.uol.com.br/*

ARAUJO - *Assunção, Marcos Flávio Araújo . Segredos do Hacker Ético.Ed. Visual Books – São Paulo, 2010*

PEDROSO - *http://www.oficinadanet.com.br/artigo/1476/termo_hacker_qual_seu_significado*

OXFORD - *http://www.askoxford.com/results/?view=dict&freesearch=hacker&branch=13842570&textsearchtype=exact*

GRUPOCSI - *http://grupocsi.blogspot.com/2008/06/footprinting.html*

CICUNB: *http://www.cic.unb.br/~pedro/trabs/buffer_overflow.htm*

BDJur
http://bdjur.stj.gov.br

VIVAOLINUX*: http://www.vivaolinux.com.br/artigo/Race-condition-vulnerabilidades-em-suids/*

LAUFER: *http://www.gta.ufrj.br/grad/03_1/sdi/index.htm*

CAPITULO III

ARTECRIATIVA*: http://www.webartigos.com/articles/16790/1/UMA-REFLEXAO-SOBRE-O-CONCEITO-DE-CRIATIVIDADE-E-O-ENSINO-DA-ARTE-NO-AMBIENTE-ESCOLAR/pagina1.html*

VYGOTSKY, L.S. *Imaginación y el arte en la infancia*. Madri: Hispanicas, 1982.

FOUCAULT(1999), *Michel, As palavras e as coisas*

CAPITULO IV

HONEYDREF *: http://www.slideshare.net/UlissesCosta/uso-de-honeypots-com-honeyd-presentation*

ASSUNÇÃO(2009): *Assunção, Marcos Flávio Araújo*. *Honeypots e Honeynets .Ed. Visual Books – São Paulo, 2009.*

BDJur
http://bdjur.stj.gov.br